A LOW PROFILE OF SECURITY USB DIGITAL DATA PROCESSING DEVICE

FIELD OF THE INVENTION

The present invention relates to a data security system using common USB interface technology and intelligent stick structure to establish a data security level as well as the one of smart cards.

BACKGROUND OF THE INVENTION

Most memory cards and authentication cards used in the current financial area are composed of a smart card system. However, the cost of establishing such system is too high, and generally such system is not supported by personal computer systems and peripherals. Therefore, a USB security authentication device is created to overcome this shortcoming, but the size and thickness of the device is larger than a regular memory card and thus not easy to carry.

SUMMARY OF THE INVENTION

The present invention discloses a USB memory card such as an intelligent stick, of which a control of data computation is included to enhance the data security and meet the data security requirements. The USB memory card of the invention is applicable to the traditional smart card market as well as featuring a low system cost and a popular USB interface. The size of such USB memory card is compact, easy-to-carry, and easy-to-use.

As to the digital data processing equipment, overcoming the above shortcomings and providing a compatible computer interface to make the application more convenient and comply with user's operating habits are important topics.

In view of the description above, the inventor of this invention based on years of experience on computer product research and marketing to conduct researches and experiments to overcome the foregoing shortcomings, and finally invented the

"A low profile of security USB digital data processing device" in accordance with this invention.

The primary objective of the present invention is to provide a security USB digital data processing device, of which a control of data encryption is included to enhance data security and meet data security requirements. The USB memory card of this invention is applicable to the traditional smart card market as well as featuring a low system cost and a popular USB interface. The size of such USB memory card is compact, easy-to-carry, and easy-to-use.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a system block diagram of the security USB digital data processing device of the present invention.

FIG. 2 is an illustrative diagram of the partition of the memory unit according to the present invention.

FIG. 3 is an illustrative diagram of the software architecture according to the present invention.

FIG. 4 is a perspective diagram of the security intelligent stick according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

To make it easier for our examiner to understand the objective of the invention, its structure, innovative features, and performance, we use a preferred embodiment together with the attached drawings for the detailed description of the invention.

Please refer to FIG. 1 for the system block diagram of the present invention, which comprises a USB controller 101 for transmitting data, a memory unit 102 electrically coupled to a circuit of said USB controller 101 for storing data, and an encryption unit 103 electrically coupled to circuits of the USB controller 101 and

memory unit 102. After a data is passed to the USB controller 101 and processed by the encryption unit 103 with a symmetric key algorithm such as DES, TDES, RC2, RC4, and RC5, etc. the data can be encrypted to be a cipher or decrypted from a cipher, and finally saved in the memory unit 102 or outputted to the external operating system.

To improve the data security level, an asymmetric key algorithm (or called as public key algorithm) is used to perform further security by encryption such as RSA, DSA, and ECC, etc. to meet the algorithm of PKI security system technology. If the power of the kernel of this encryption unit is enough, hash algorithm also can be achieved, like as MD2, MD5 or SHA, etc. A random number generator 104 is implemented into the system to facilitate and enhance the design of security. The random number generator 104 produces a random number as a key for the foregoing encryption. Such arrangement can further improve the data security.

To meet the requirements of the hardware operation as shown in FIG. 1, an appropriate application program interface (API) must be provided for system developers to call it and develop her security operating system.

Besides the capability of the hardware encryption, the design of this invention also focuses on dividing the memory unit into a plurality of blocks with different features. The types of blocks include general block, read only block, and reserved block. The general block is provided for end users to save, modify and read the data to or from this memory block, The read only block is provided for end users to read data, but does not allow end users to write, delete, or modify data unless the end user has gone through an authentication procedure such as entering a correct password. The reserved block does not allow general end users to read, write, modify, delete data, or even format the device or this memory block. The data in the reserved block is reserved for specific system service providers. By the foregoing application program interface (API), data can be accessed from the reserved block at a far end via internet, which can further improve the security level of the USB memory card of this invention. Such hardware feature of dividing the memory into

blocks is not found in traditional smart cards yet.

Please refer to FIG. 2 for the illustration of the division of a memory unit 200 of the present invention. The memory unit 200 is divided into a general block 201, a read only block 202, and a reserved block 203.

Please refer to FIG. 3 for the software architecture of the present invention. This software architecture includes a physical layer 301 which adopts an intelligent stick of a USB memory card for the hardware design, a driving layer 302 for calling the subroutine for the data processing between a host system and the physical layer and handling the request for processing the application at the upper layer to this device which could meet the Microsoft PC/SC specifications, a user interface layer 303 which could satisfy the PKCS#11 standard interface or Microsoft CryptoAPI interface specifications, and an application layer 304 which is the high-level application interface (API) providing programmers a familiar programming interface for the system development.

A low-cost, low profile, light, thin, short, and compact security USB memory device can be made according to the system block diagram of FIG. 1 and the software architecture as shown in FIG. 3. Further, an intelligent stick as shown in FIG. 4 can be used to commercialize the invention into a security intelligent stick.

By means of the design of the USB security operating system according to this invention, users do not need to purchase an expensive smart card reader, and thus greatly reducing costs as well as getting more convenience in PC platform. Further, the utilization of intelligent stick can reduce the size of the device to card form factor and need no adapter to transfer USB signal as connecting to a standard USB port thus bring us convenience and portability.

In summation of the above description, the present invention enhances the performance of the conventional structure, and further complies with the patent application requirements and is submitted to the Patent and Trademark Office for review and granting of the commensurate patent rights.

While the invention has been described by way of example and in terms of a preferred embodiment, it is to be understood that the invention is not limited thereto. To the contrary, it is intended to cover various modifications and similar arrangements and procedures, and the scope of the appended claims therefore should be accorded the broadest interpretation so as to encompass all such modifications and similar arrangements and procedures.